

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of)	
)	
Implementation of the Telecommunications Act)	CC Docket No. 96-115
1996;)	
)	
Telecommunications Carriers' Use of Customer)	
Proprietary Network Information and Other)	
Customer Information;)	
)	
Petition for Rulemaking to Enhance Security and)	RM-11277
Authentication Standards for Access to Customer)	
Proprietary Network Information)	

**COMMENTS OF
US LEC CORP.**

US LEC Corp., on behalf of itself and its operating subsidiaries (collectively ("US LEC"), submits its comments in response to the Notice of Proposed Rule Making adopted by the Commission in the above-styled proceeding. US LEC, like all telecommunications carriers, is committed to safeguarding its customers' proprietary network information ("CPNI") and takes seriously its obligations to keep the CPNI protected from unauthorized disclosure. US LEC supports the Commission in taking action to ensure that all telecommunications carriers comply with the CPNI rules, but cautions the Commission in adopting such stringent rules that inconveniences the customers who make valid requests to obtain information on their CPNI. In addition, certain of the proposed "cures" may be result in additional costs being imposed on a carrier which may then need to be passed on to the customer in the form of rate increases. Accordingly, the Commission must

adopt rules that carefully balance the privacy concerns of the customer with the cost of additional security measures that may be imposed.

Currently, US LEC has not identified any efforts by the so-called data brokers to obtain CPNI for US LEC customers. Consequently, US LEC is unable to provide any additional information to the Commission on the nature or the scope of the problem that EPIC identified in its petition for rule making. Nevertheless, US LEC is concerned with certain of the measures that the Commission is considering in the Notice, which may keep CPNI secure, but may result in increased costs to US LEC to implement the proposed measures into its systems and may result in customers not having convenient access to their account records. US LEC provides telecommunications services to business customers, although it does provide a Voice over Internet Protocol (“VoIP”) service through one of its subsidiaries that provides services to residential customers. Below are US LEC's comments on certain of the suggested measures to protect CPNI:

Consumer set passwords

With business customers, US LEC generally has one point of contact with a customer who is authorized to request information on an account or make changes to the account. In some instances, there may be more than one contact depending on the customer's desires. US LEC does provide a web-based tool that allows its customers to review their bills and make certain changes to their account. The customer is provided a US LEC-set password initially, but then the customer may re-set the password (and is encouraged to do so). Once the customer re-sets the

password, then should the customer misplace or forget the password, the customer must call US LEC and, after certain security questions being asked, US LEC will re-set the password.

Even with customer set passwords, there is no guarantee that the CPNI is safe and secure. Many customers may use passwords that (1) are easily hacked; (2) may be available in a publicly available space or file; or (3) are provided to a number of persons within the company, who may not hold the password secure. In some instances, the customer may be working with a telecom consultant or agent, and provides the customer password to that third party, which may also not protect access to the password. Moreover, an unauthorized third party may attempt to change a password by calling the carrier because of a “lost” password. Although there are security questions that may be used to ensure that the carrier is speaking to the authorized person for that customer account, if the third party has done his/her homework, these questions may be insufficient to determine that the person is unauthorized.

One measure to combat the attempt to change a password by an unauthorized person is to send an email or other notification to the customer that the password has been changed. As long as the customer has kept its current information updated, the email is not caught in a spam filter, and the email is actually read by the customer, this is a means to catch the unauthorized change. Again there is no guaranteed method to ensure that the customer is aware of the change of a password – it is again dependent on the diligence of the customer.

Consequently, US LEC does not believe that a Commission rule mandating customer set passwords to be used to access CPNI will make the information any more secure. US LEC believes that the use of a password protected accounts should be at the discretion of the carrier, and that the carrier should decide on what the best means is to keep the password and account secure based on its system and processes.

Audit Trails

EPIC suggested that each carrier record all instances when a customer's records have been accessed, whether the information was disclosed, and to whom. Under the existing Commission rules, US LEC is required, and does, record access of the CPNI for its own marketing purposes and pursuant to a request of a third party. US LEC's systems and processes are set up to retain this information. On the other hand, if US LEC were required to record every time a customer's record was accessed (whether the access was by the customer through the web-based tool or by US LEC's employees during the ordinary course of business to maintain the account), it would be burdensome and not beneficial. Not only would US LEC have to change its systems and processes to make such recordings, it would then have to maintain the records for some length of time. US LEC opposes any additional recording requirements beyond the existing requirements.

Encryption

US LEC disagrees with EPIC that a mandated encryption of data stored by the carrier will have any affect on the unauthorized access of CPNI. Requiring US

LEC to encrypt its data will cause undue cost and burden on it, without any corresponding benefit or security of the data. To access the CPNI data that US LEC has in its database, the person must either go through US LEC personnel to obtain the CPNI or use a customer available access site. Accordingly, US LEC opposes the adoption of mandated encryption.

Limiting Data Retention

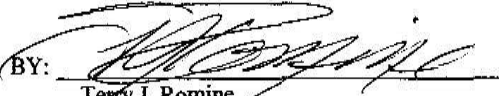
EPIC has suggested that call records should be deleted when they are no longer needed for billing or dispute purposes, or “deidentify” records so that the separate data that identifies the caller from the general transactions records is deleted. Today most carriers have a record retention policy that incorporates the Commission’s Part 42 record-keeping requirements or requirements under the Sarbanes-Oxley Act. Thus, a Commission-imposed time period that limits a carrier’s ability to retain records may conflict with other requirements under federal laws and rules and regulations. Also if a carrier is required to delete a call record that it believes is no longer needed for billing or dispute purposes, then there must be a corresponding rule that states if the carrier deletes the record after a reasonable period of time pursuant to the Commission’s rule, the customer is thereafter foreclosed from disputing the charges associated with the deleted records. US LEC does not believe that a limitation on data retention will provide any greater protection to CPNI and would be adverse to the consumer.

Conclusion

US LEC agrees that each carrier must address and meet its obligations to protect CPNI of its customers. Nevertheless, the measures taken should not adversely affect the customer, by making it more difficult and time consuming to access information about their account, nor should it add significant costs to the carriers by requiring them to revamp their systems and processes to meet the obligations.

Respectfully submitted,

US LEC CORP.

BY: 
Terry J. Romine
Deputy General Counsel – Regulatory
US LEC
6801 Morrison Boulevard
Charlotte, NC 28211
(704) 319-1119 (Direct dial)
(704) 602-1119 (Fax)
tromine@uslec.com

Date: April 28, 2006